A-1.
サイバー攻撃および防御についての基本的知識と演習

公益社団法人　私立大学情報教育協会

セッションの目的

サイバー攻撃および防御に関するインシデントを、
基礎的なサイバーレンジ演習で体験する

セキュリティインシデントへの対応手法を学び
基本的な対処法や役割を理解して対策が取れるようにする

公益社団法人　私立大学情報教育協会

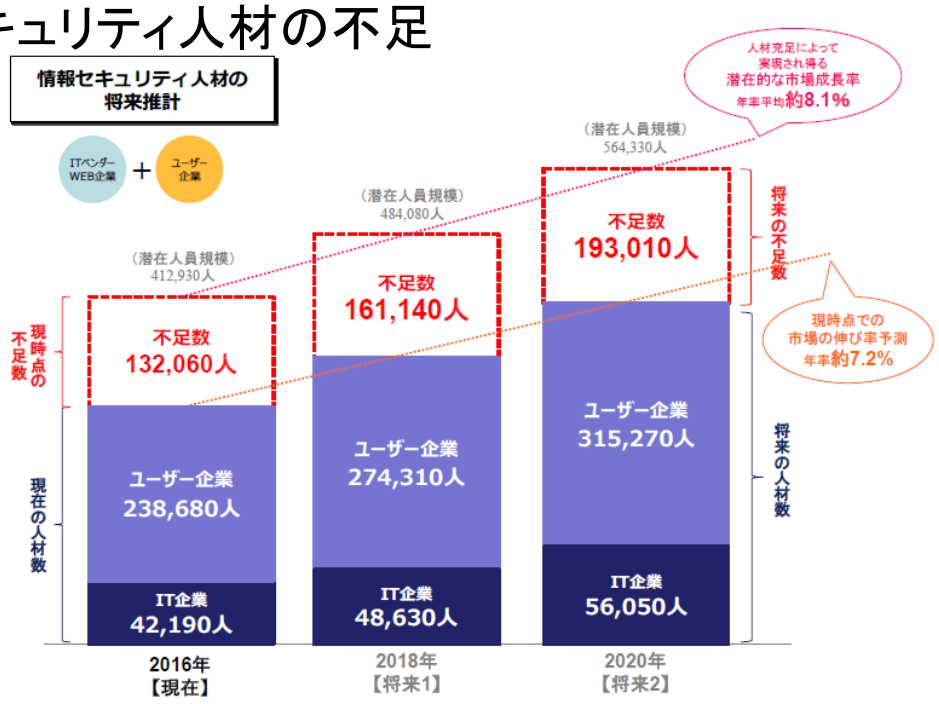
メニュー

1. セキュリティ人材
    1. セキュリティ人材の育成
    2. サイバーレンジ
2. SOCとCSIRT
3. 演習
    1. 攻撃フェイズ
    2. 防御フェイズ
    3. インシデント報告書
    4. 対策の立案

セキュリティ人材

セキュリティ人材育成の状況

■ セキュリティ人材の不足



公益社団法人　私立大学情報教育協会

セキュリティ人材育成の状況

■ セキュリティ人材の教育

種類	目的	実施方法例
講義・セミナー	啓発・認知・意識共有	脅威や対策の動向の授業や講演・研修など
ワークショップ	対応確認・相互理解	インシデント対応計画や手順の確認・議論
模擬訓練	計画や手順の検証・評価	インシデント発生時の対応の妥当性の確認・議論
ゲーム演習	決定・判断の検証・手法の発掘	ゲーム形式での対応・判断、効果的な対応の検討
総合演習	総合的な対応力向上	現実の環境に近い実践体な対応・手段の確認

準備　・目的、課題の把握　・シナリオ作成　・演習環境構築

実施　・参加者への説明　・演習実施　・意見交換

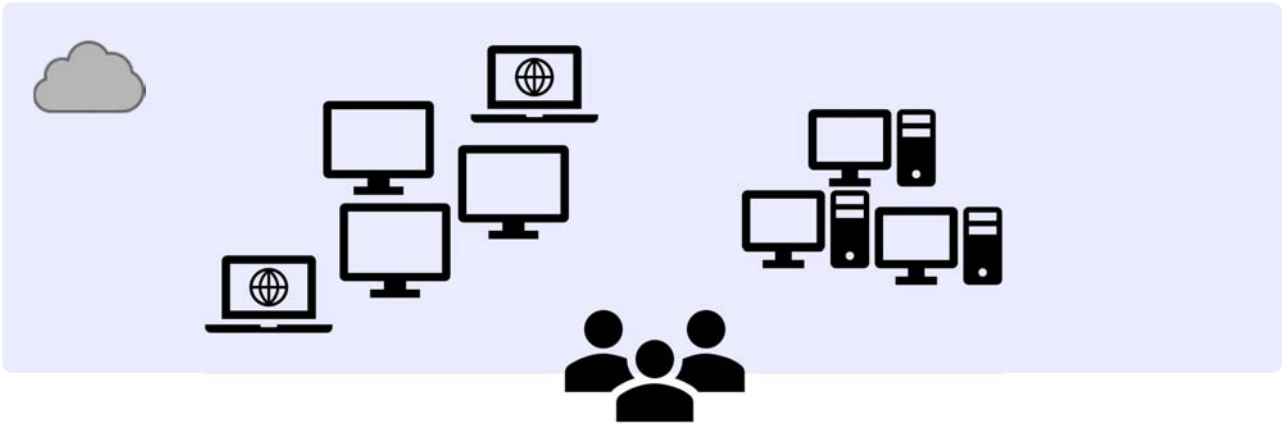
評価　・演習結果の整理　・分析、評価

公益社団法人　私立大学情報教育協会

サイバーレンジ

- サイバーレンジとは
  - 実世界を模した仮想システム環境
  - 実際に使われている機器やアプリケーション
  - 本物のマルウェア

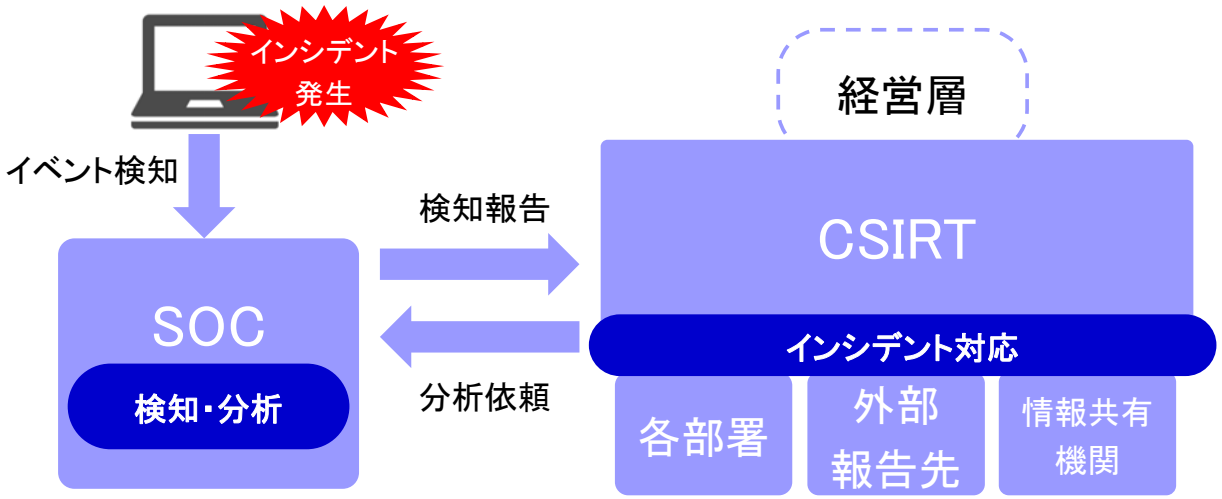
これらを用いた**実践的演習環境**



SOCとCSIRT

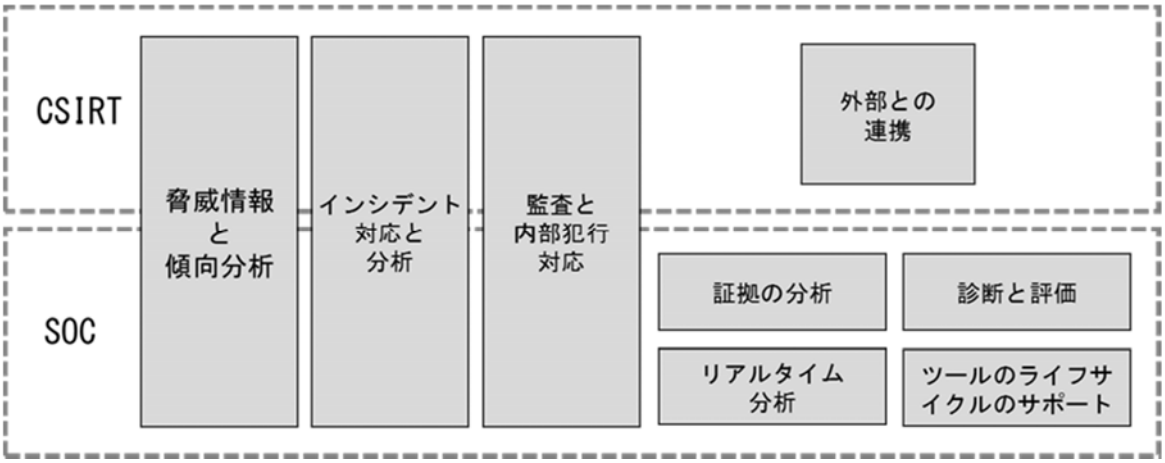
SOCとCSIRT

- サイバーセキュリティの組織体制
  - SOC（Security Operation Center）
  - CSIRT（Computer Security Incident Response Team）



SOCとCSIRT

- SOCとCSIRTの機能分担



SOCとCSIRT

■ SOCの役割

機能	役割
リアルタイム分析	コールセンター、NWログ分析、PCAPログ分析、トリアージ情報収集等 監視の結果からリアルタイムで対応を決定する
脅威情報と傾向分析	脅威情報の収集・分析、定期レポートの生成、対策への組み込み等 脅威情報を取り扱う
インシデント対応と分析	オンサイトやリモートでのインシデント対応、インシデント分析、侵入手口の分析、監督官庁との連携、インシデントクローズ報告等インシデント対応の実施
インシデント：証拠の分析	フォレンジックの証拠の取り扱いと分析、マルウェアの分析等 得られた証拠の分析を行う
ツールのライフサイクルのサポート	監視設備（センサ以外も含む）のメンテナンス、インシデント対応製品導入支援、センサーのチューニングと維持管理（IDS,IPS,SIEMなど）、カスタムシグネチャの作成、ツールの開発支援等利用するツールの開発や維持管理を行う
監査と内部犯行対応	監査データの収集と配布、内部犯行事案の調査等監査と内部犯行についての対応を行う
診断と評価	脆弱性診断、侵入テスト、脆弱性の評価等脆弱性診断により評価を実施する
外部との連携	製品の評価、メディア対応の窓口支援、研修や啓発、外部への脅威情報の公開等 社内外との対応を行う

SOCとCSIRT

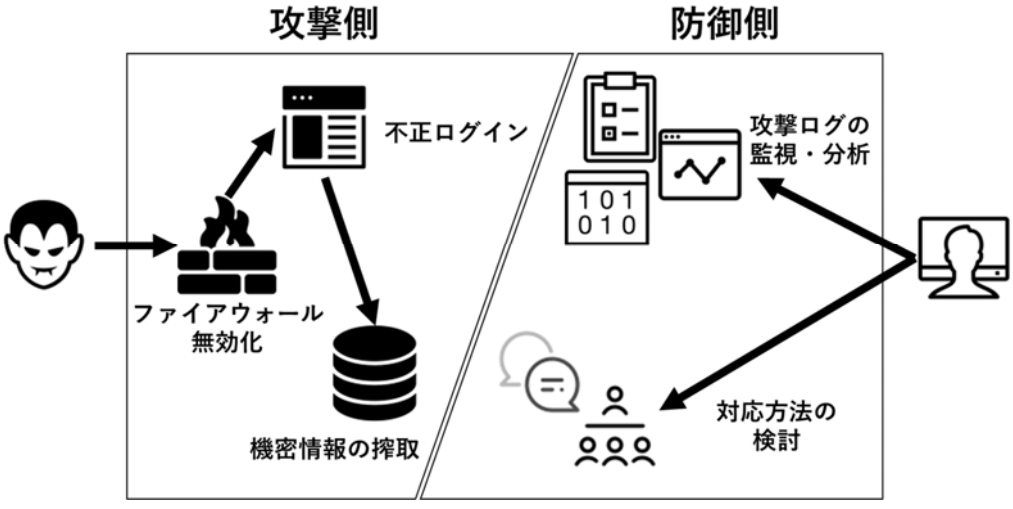
■ CSIRTの役割

機能	役割	業務内容
情報共有	PoC（Point of Contact）	組織内の各部署や組織外との連絡、IT部門との調整
	リーガルアドバイザー（法務担当）	法課題やコンプライアンス問題が発生した時の法的アドバイス
	ノーティフィケーション	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー（情報収集担当）、 キュレーター（情報分析担当）	インシデントの情報収集、各種情報に対する分析、国際情勢の把握、 自組織への適用検討
	脆弱性診断士	OS、ネットワーク、アプリケーションの脆弱性評価
	セルフアセスメント	平時のリスクアセスメント、有事の際の脆弱性の分析、影響の調査
	ソリューションアナリスト	セキュリティ戦略としてのFiT&Gap分析、リスク評価、 有事の際の有効性評価
インシデント対応	コマンダー（CSIRT全体統括）	意思決定、社内PoC、役員、CISO、または経営層との情報連携
	インシデントマネージャー （インシデント管理担当）	インシデント管理 インシデントの対応状況の把握、コマンダーへの報告、対応履歴把握
	インシデントハンドラー （インシデント処理担当）	インシデント現場監督、セキュリティベンダーとの連携
	インベスティゲーター （調査・捜査担当）	捜査に必要な論理的思考、分析力、自組織内システム理解力を使った 内偵
	トリアージ（優先順位選定担当）	事象に対する優先順位の決定
	フォレンジック	証拠保全、システム的な鑑識、足跡追跡、マルウェア解析
自組織内教育	教育担当	自組織内のリテラシー向上、底上げ

演習

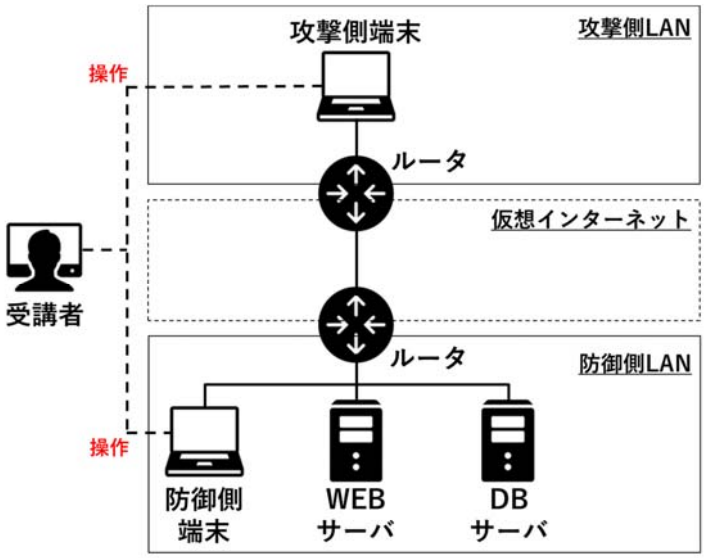
演習環境

- シナリオ「Webサーバへの不正アクセス」
  - 攻撃と防御の基礎
  - 個別のPCに演習環境を構築



演習環境

- 演習環境の構成
  - 操作はホスト側のブラウザから実行
  - 演習環境はVirtualBox仮想マシン内にDockerコンテナで構築



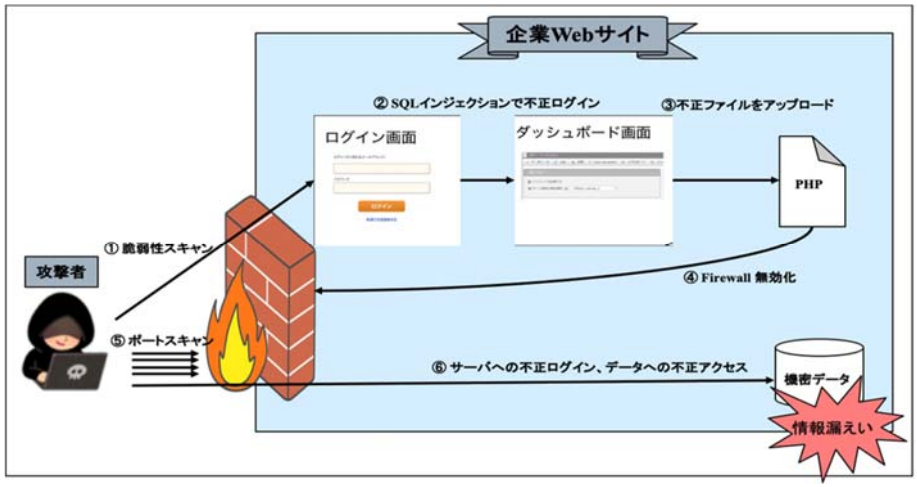
演習環境

- 演習で取り扱う主な脆弱性
  - SQLインジェクション
    不正な文字列をサーバに送信することで、
    SQLのクエリ構文を無理やり変更させる。
    これにより以下の不正行為が可能
    ・認証処理の回避
    ・DBへの不正アクセス
  - ファイルアップロード機能の不備
    不正なスクリプトファイルをサーバにアップロードし、
    そのファイルにアクセスすることでスクリプトを実行
    これにより以下の不正行為が可能
    ・サーバの設定変更、バックドアの設置
    ・他のサーバに対する攻撃の踏み台として利用

演習内容

■ 攻撃フェイズの演習概要

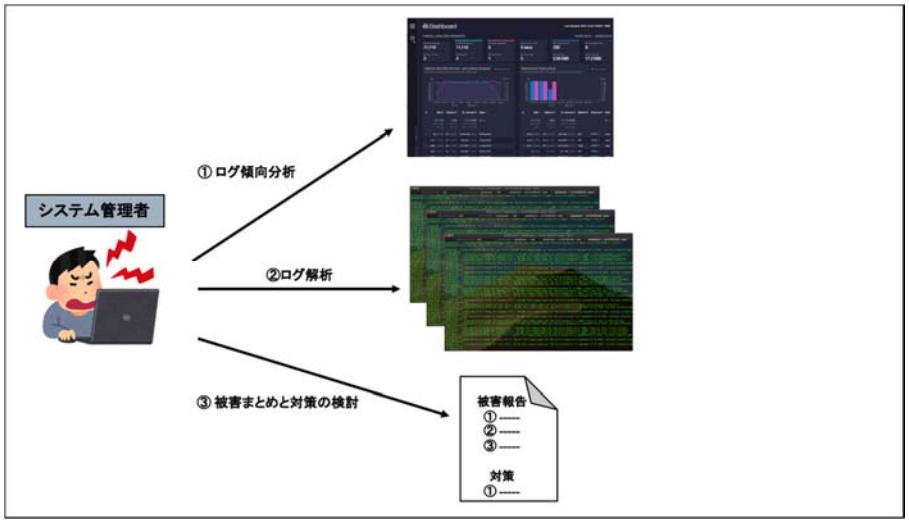
1. グループウェアを想定したWebアプリケーションに対して脆弱性スキャンを実施
2. スキャン結果をもとに、SQLインジェクション攻撃を実施、Webアプリケーションへ不正ログイン
3. Webアプリケーションのファイルアップロード機能を悪用、不正なphpファイルをアップロード
4. スクリプトを実行、バックドアを設置
5. ポートスキャンを行い、設置したバックドアへアクセスできるポートを調査
6. バックドアからWebサーバへ不正ログイン、企業情報を不正取得



演習内容

■ 防御フェイズの演習概要

1. ログ分析ツールを確認、ログの傾向から不正アクセスの可能性を判断
2. Webサーバのログを調査、不正侵入の痕跡および侵入経路を調査
3. 調査結果から想定できる被害の推定および対策の検討を実施



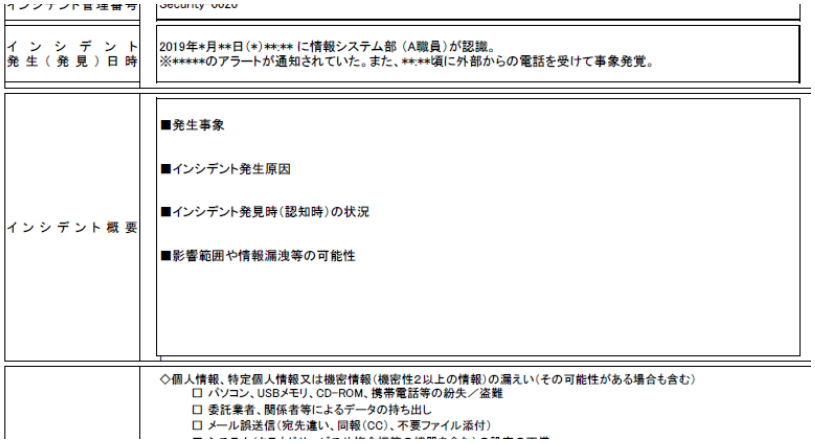
演習内容

- インシデント報告書の作成

起こった攻撃や検知・調査の内容を明確に記載

- 再発防止策の策定

今回の攻撃を防ぐ・被害を抑えるために有効な対策は？
（システム的・組織体制的な対策）



インシデント管理番号	Security-0020
インシデント発生（発見）日時	2019年*月**日（*）**:** に情報システム部（A職員）が認識。 ※*****のアラートが通知されていた。また、**:**頃に外部からの電話を受けて事象発覚。
インシデント概要	■発生事象 ■インシデント発生原因 ■インシデント発見時（認知時）の状況 ■影響範囲や情報漏洩等の可能性
	◇個人情報、特定個人情報又は機密情報（機密性2以上の情報）の漏えい（その可能性がある場合も含む） □ パソコン、USBメモリ、CD-ROM、携帯電話等の紛失／盗難 □ 委託業者、関係者等によるデータの持ち出し □ メール誤送信（宛先違い、同報（CC）、不要ファイル添付）

演習内容

- SQLインジェクション対策の例

対策	概要
サーバ対策	SQL文を成立させないエスケープ処理の実装 入力エリアの文字数制限
ネットワーク対策	WAF(Webアプリケーションファイアウォール)導入
WEBの脆弱性対策	脆弱性診断やの実施、診断サービスの利用
導入時の対策	セキュアなコーディング 仕様書などによる脆弱性対策の確認

A-1 おわりに

- サイバーレンジを使った演習の意義

・実際の攻撃手法やマルウェアなどの体験を通して
実践的な対処方法を学べる

・役割に応じた行動を意識し、インシデント対応の
訓練が実施できる

・様々なレベルや学習内容のシナリオを通して、
システム担当以外にもCSIRT構成員の教育が可能

参考文献

1．経済産業省委託事業：みずほ総研株式会社
「IT ベンチャー等によるイノベーション促進のための
人材育成・確保モデル事業」事業報告書　第2部
https://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_fullreport.pdf

2．瀬戸洋一、中田亮太郎ほか
「情報セキュリティ概論」翔泳社、2019年

3．マカフィー株式会社：SQLインジェクション攻撃への対策
https://blogs.mcafee.jp/sql-injection-prevention

4．トレンドマイクロ株式会社：2019年度　文部科学省
サイバーセキュリティ人材育成に関する研修資料